CLAIMS

[1] An information distribution system including a distribution device for distributing a content and a terminal device for receiving the content distributed from the distribution device, wherein:

the distribution device transmits information regarding a PKI-related information acquisition instruction for requesting the terminal device to acquire latest PKI-related information together with information required for using the content; and

the terminal device, when receiving the PKI-related information acquisition instruction transmitted from the distribution device, acquires the latest PKI-related information.

[2] An information distribution system according to claim 1, wherein:

the distribution device includes a PKI-related information acquisition instruction broadcast unit operable to broadcast information regarding the PKI-related information acquisition instruction for requesting the terminal device to acquire the latest PKI-related information together with the information required for using the content; and

the terminal device includes a PKI-related information acquisition unit operable to acquire the latest PKI-related information when receiving the information regarding the

PKI-related information acquisition instruction which is broadcast.

[3] An information distribution system according to claim 1, wherein:

the distribution device includes:

a PKI-related information broadcast unit operable to broadcast PKI-related information as being multiplexed to a broadcast signal; and

a PKI-related information acquisition instruction transmission unit operable to transmit, to the terminal device via communication, the information regarding the PKI-related information acquisition instruction for requesting the terminal device to acquire the latest PKI-related information together with the information required for using the content; and

the terminal device includes a PKI-related information acquisition unit operable to acquire the PKI-related information which is broadcast when the information regarding the PKI-related information acquisition instruction is transmitted from the distribution device.

[4] An information distribution system according to claim 2, wherein:

the distribution device further includes a PKI-related information transmission unit operable to transmit the latest

PKI-related information via a communication network in response to the request from the PKI-related information acquisition unit; and

the PKI-related information acquisition unit receives the latest PKI-related information transmitted from the distribution device.

[5] An information distribution system according to claim 4, wherein the PKI-related information transmission unit transmits the latest PKI-related information as being included in a message of a SAC (Secure Authenticated Channel) protocol.

[6] An information distribution system according to claim 4, wherein the PKI-related information acquisition instruction broadcast unit broadcasts a connection destination for acquiring the latest PKI-related information via communication together with the information regarding the PKI-related information acquisition instruction.

[7] An information distribution system according to claim 2, wherein:

the distribution device further includes a PKI-related information broadcast unit operable to broadcast the PKI-related information as being multiplexed to a broadcast signal; and

the PKI-related information acquisition unit acquires

the latest PKI-related information broadcast as being multiplexed to the broadcast signal based on the PKI-related information acquisition instruction which is broadcast.

[8] An information distribution system according to claim 7, wherein the PKI-related information broadcast unit broadcasts the PKI-related information as being included in a private section of MPEG-2 Systems.

[9] An information distribution system according to claim 7, wherein the PKI-related information broadcast unit broadcasts the PKI-related information as being included in a data carousel.

[10] An information distribution system according to claim 7, wherein the PKI-related information acquisition instruction broadcast unit broadcasts an acquisition source through which the latest PKI-related information is acquired via broadcast together with the information regarding the PKI-related information acquisition instruction.

[11] An information distribution system according to claim 2, wherein the PKI-related information acquisition instruction broadcast unit broadcasts the information regarding the PKI-related information acquisition instruction as being included in an ECM (Entitlement Control Message: common information) or

an EMM (Entitlement Management Message: individual information) and as being multiplexed to the ECM or the EMM.

[12] An information distribution system according to claim 2, wherein:

the information regarding the PKI-related information acquisition instruction is a flag indicating the PKI-related information acquisition instruction; and

the PKI-related information acquisition unit refers to the flag to determine whether or not to acquire the latest PKI-related information.

[13] An information distribution system according to claim 2, wherein:

the information regarding the PKI-related information acquisition instruction is either an expiration time, a creation time and date, a version, a size or a number of certificate entries of the PKI-related information, or a combination thereof; and

the PKI-related information acquisition unit determines whether or not to acquire the latest PKI-related information by comparing either the expiration time, the creation time and date, the version, the size or the number of certificate entries of the PKI-related information stored in the terminal device or a combination thereof with the information regarding the PKI-related information acquisition instruction.

[14] An information distribution system according to claim 13, wherein the PKI-related information acquisition unit, when determining that the PKI-related information has been updated as a result of the comparison, acquires the latest PKI-related information.

[15] An information distribution system according to claim 2, wherein the PKI-related information is a CRL (Certificate Revocation List).

[16] An information distribution system according to claim 2, wherein the PKI-related information is a public key certificate.

[17] An information distribution system according to claim 2, wherein:

the distribution device further includes a PKI-related information update determination unit operable to determine whether or not the PKI-related information stored therein has been updated; and

the PKI-related information acquisition instruction broadcast unit, when the PKI-related information update determination unit determines that the PKI-related information has been updated, broadcasts the information regarding the PKI-related information acquisition instruction together with the

information required for using the content.

[18] An information distribution system according to claim 3, wherein the PKI-related information acquisition instruction transmission unit transmits the information regarding the PKI-related information acquisition instruction as being included in a message of a SAC protocol to the terminal device.

[19] An information distribution system according to claim 18, wherein the PKI-related information acquisition instruction transmission unit includes the information regarding the PKI-related information acquisition instruction in a license transmitted via the SAC protocol.

[20] An information distribution system according to claim 3, wherein the PKI-related information broadcast unit broadcasts the PKI-related information as being included in a private section of MPEG-2 Systems.

[21] An information distribution system according to claim 3, wherein the PKI-related information broadcast unit broadcasts the PKI-related information as being included in a data carousel.

[22] An information distribution system according to claim 3, wherein the PKI-related information acquisition instruction

transmission unit transmits an acquisition source through which the latest PKI-related information is acquired via broadcast together with the information regarding the PKI-related information acquisition instruction.

[23] An information distribution system according to claim 3, wherein:

the information regarding the PKI-related information acquisition instruction is a flag indicating the PKI-related information acquisition instruction; and

the PKI-related information acquisition unit refers to the flag to determine whether or not to acquire the latest PKI-related information.

[24] An information distribution system according to claim 3, wherein:

the information regarding the PKI-related information acquisition instruction is either an expiration time, a creation time and date, a version, a size or a number of certificate entries of the PKI-related information, or a combination thereof; and

the PKI-related information acquisition unit determines whether or not to acquire the latest PKI-related information by comparing either the expiration time, the creation time and date, the version, the size or the number of certificate entries of the PKI-related information stored in the terminal

device or a combination thereof with the information regarding the PKI-related information acquisition instruction.

[25] An information distribution system according to claim 24, wherein the PKI-related information acquisition unit, when determining that the PKI-related information has been updated as a result of the comparison, acquires the latest PKI-related information.

[26] An information distribution system according to claim 3, wherein the PKI-related information is a CRL.

[27] An information distribution system according to claim 3, wherein the PKI-related information is a public key certificate.

[28] An information distribution system according to claim 3, wherein:

the distribution device further includes a PKI-related information update determination unit operable to determine whether or not the PKI-related information stored therein has been updated; and

the PKI-related information acquisition instruction transmission unit, when the PKI-related information update determination unit determines that the PKI-related information has been updated, transmits the information regarding the

PKI-related information acquisition instruction together with the information required for using the content.

[29] A terminal device for receiving a content distributed from a distribution device, wherein the terminal device acquires latest PKI-related information when receiving, together with information required for using the content, information regarding a PKI-related information acquisition instruction for requesting the terminal device to acquire the latest PKI-related information transmitted from the distribution device.

[30] A terminal device according to claim 29, which comprises:

a PKI-related information acquisition instruction receiving unit operable to receive the information regarding the PKI-related information acquisition instruction for requesting acquisition of the latest PKI-related information which is broadcast as being multiplexed to a broadcast signal; and

a PKI-related information acquisition unit operable to acquire PKI-related information which is broadcast from the distribution device when the PKI-related information acquisition instruction receiving unit receives, together with the information required for using the content, the information regarding the PKI-related information acquisition instruction.

[31] A terminal device according to claim 29, which comprises:

a PKI-related information acquisition instruction receiving unit operable to receive the information regarding the PKI-related information acquisition instruction which is transmitted from the distribution device via communication; and

a PKI-related information acquisition unit operable to acquire PKI-related information which is broadcast from the distribution device when the PKI-related information acquisition instruction receiving unit receives, together with the information required for using the content, the information regarding the PKI-related information acquisition instruction.

[32] A terminal device according to claim 29, which comprises:

a PKI-related information acquisition instruction receiving unit operable to receive the information regarding the PKI-related information acquisition instruction for requesting acquisition of the latest PKI-related information which is broadcast; and

a PKI-related information acquisition unit operable to acquire the latest PKI-related information from the distribution device via communication when the PKI-related information acquisition instruction receiving unit receives the information regarding the PKI-related information acquisition instruction.

[33] A distribution device for distributing a content to a terminal device, wherein the distribution device transmits,

together with information required for using the content, information regarding a PKI-related information acquisition instruction for requesting the terminal device to acquire latest PKI-related information.

[34] A distribution device according to claim 33, which comprises:

a PKI-related information broadcast unit operable to broadcast PKI-related information as being multiplexed to a broadcast signal; and

a PKI-related information acquisition instruction broadcast unit operable to broadcast, together with the information required for using the content, the information regarding the PKI-related information acquisition instruction for requesting the terminal device to acquire the latest PKI-related information.

[35] A distribution device according to claim 33, which comprises:

a PKI-related information broadcast unit operable to broadcast PKI-related information as being multiplexed to a broadcast signal; and

a PKI-related information acquisition instruction transmission unit operable to transmit, together with the information required for using the content, the information regarding the PKI-related information acquisition instruction for

requesting the terminal device to acquire the latest PKI-related information, to the terminal device via communication.

[36] A distribution device according to claim 33, which comprises a PKI-related information acquisition instruction broadcast unit operable to broadcast the information regarding the PKI-related information acquisition instruction for requesting the terminal device to acquire the latest PKI-related information, and causes the terminal device to acquire the latest PKI-related information via communication.